

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.1
BẮT VÀ PHÂN TÍCH GÓI TIN TRONG MẠNG**

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH.....	3
1.1 Mục đích.....	3
1.2 Lý thuyết bài thực hành.....	3
1.2.1 Sniffer là gì?	3
1.2.2 Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Tcpdump	3
1.2.3 Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Wireshark	4
1.2.4 Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Network Miner	5
CHƯƠNG 2. nội dung bài thực hành.....	6
2.1 Chuẩn bị môi trường	6
2.2 Các bước thực hiện.....	8
2.2.1 Sử dụng tcpdump để bắt gói tin	8
2.2.2 Sử dụng Wireshark để phân tích gói tin trên dải mạng 192.168.100.0	11
2.2.3 Sử dụng Wireshark để phân tích gói tin trên dải mạng 10.10.19.0	12
2.2.4 Sử dụng Network Miner để phân tích gói tin.....	13
KẾT LUẬN	16
TÀI LIỆU THAM KHẢO.....	16

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách thức bắt dữ liệu mạng, bao gồm:

- Sử dụng tcpdump để bắt gói tin mạng
- Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP)
- Sử dụng Network Miner để bắt và phân tích gói tin mạng

1.2 Lý thuyết bài thực hành

1.2.1 Sniffer là gì?

Sniffer hay packet sniffer là một chương trình phần mềm nghe trộm gói tin (còn gọi là chương trình phân tích mạng, phân tích giao thức hay nghe trộm Ethernet), có khả năng chặn bắt và ghi lại lưu lượng dữ liệu qua một mạng viễn thông số hoặc một phần của một mạng. Khi các dòng dữ liệu di chuyển qua lại trong một mạng, chương trình sẽ chặn bắt các gói tin rồi giải mã và phân tích nội dung của nó theo đặc tả RFC hoặc các đặc tả thích hợp khác.

Tùy theo cấu trúc mạng (hub hay chuyển mạch) mà có thể nghe trộm tất cả hoặc chỉ một phần lưu lượng dữ liệu qua lại từ một máy trong mạng. Đối với mục đích giám sát mạng (network monitoring), có thể theo dõi tất cả các gói tin trong một mạng LAN bằng cách sử dụng một thiết bị chuyển mạch với một cổng theo dõi (lắp lại tất cả các gói tin đi qua các cổng của thiết bị chuyển mạch).

1.2.2 Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Tcpdump

Tcpdump là một công cụ dòng lệnh được sử dụng để ghi lại và phân tích gói tin trên mạng. Nó cho phép bạn theo dõi lưu lượng mạng đi qua một giao diện cụ thể trên hệ thống của bạn. Bằng cách sử dụng các cú pháp và tùy chọn khác nhau, bạn có thể lọc và hiển thị các gói tin theo nhiều tiêu chí khác nhau như địa chỉ IP, cổng, giao thức, và nhiều hơn nữa. Tcpdump là một công cụ mạnh mẽ được sử dụng rộng rãi trong quản trị hệ thống và mạng để chẩn đoán và gỡ lỗi vấn đề liên quan đến mạng.

Tcpdump sẽ giúp bạn phân các gói dữ liệu phù hợp với dòng lệnh mang theo, cụ thể:

- Bắt bản tin và lưu bằng định dạng PCAP (có thể đọc bởi wireshark)
- Nhìn thấy trực tiếp các bản tin điều khiển hệ thống Linux sử dụng wireshark, xem chi tiết remote packet capture using Wireshark và tcpdump
- Có thể nhìn thấy các bản tin trên DUMP trên terminal
- Tạo các bộ lọc Filter để bắt bản tin cần thiết như: http, ssh, ftp...
- Ngoài ra tcpdump còn sử dụng nhiều option khác nhau nữa

Định dạng chung của một dòng giao thức tcpdump:

time-stamp src > dst: flags data-seqno ack window urgent options

Trong đó:

- Time-stamp: hiển thị thời gian gói tin được capture.
- Src và dst: hiển thị địa IP của người gửi và người nhận.
- Cờ Flag thì bao gồm các giá trị sau:
 - S(SYN): Được sử dụng trong quá trình bắt tay của giao thức TCP.
 - (ACK): Được sử dụng để thông báo cho bên gửi biết là gói tin đã nhận được dữ liệu thành công.
 - F(FIN): Được sử dụng để đóng kết nối TCP.
 - P(PUSH): Thường được đặt ở cuối để đánh dấu việc truyền dữ liệu.
 - R(RST): Được sử dụng khi muốn thiết lập lại đường truyền.
- Data-seqno: Số sequence number của gói dữ liệu hiện tại.
- ACK: Mô tả số sequence number tiếp theo của gói tin do bên gửi truyền (số sequence number mong muốn nhận được).
- Window: Vùng nhớ đệm có sẵn theo hướng khác trên kết nối này.
- Urgent: Cho biết có dữ liệu khẩn cấp trong gói tin.

TCPdump là một công cụ dòng lệnh được sử dụng để theo dõi và phân tích gói tin trên mạng. Nó hoạt động bằng cách lắng nghe và ghi lại các gói tin mạng đang đi qua một giao diện mạng cụ thể trên một máy tính. Khi được chạy, TCPdump sẽ hiển thị thông tin về các gói tin này, bao gồm địa chỉ nguồn và đích, loại giao thức, dữ liệu payload, và nhiều thông tin khác. Người dùng có thể sử dụng các tùy chọn và bộ lọc để tinh chỉnh việc theo dõi và phân tích theo nhu cầu cụ thể của họ.

1.2.3 Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Wireshark

Wireshark là một công cụ phân tích gói tin mạng mạnh mẽ và đa năng. Nó cho phép bạn chụp, xem xét và phân tích gói tin trên mạng. Wireshark hỗ trợ nhiều loại giao thức mạng và cung cấp các tính năng như lọc gói tin, phân tích luồng dữ liệu, và đồ thị hoạt động mạng. Công cụ này thường được sử dụng để chẩn đoán và gỡ lỗi vấn đề liên quan đến mạng, cũng như để nghiên cứu bảo mật mạng và kiểm tra hiệu suất mạng. Wireshark có giao diện đồ họa dễ sử dụng và được hỗ trợ trên nhiều hệ điều hành khác nhau.

Wireshark là một phần mềm dùng để phân tích và giám sát lưu lượng mạng. Dưới đây là một số chức năng chính của Wireshark:

- Phân tích Gói Tin: Wireshark cho phép bạn theo dõi và phân tích từng gói tin dữ liệu trên mạng. Bạn có thể xem các thông tin chi tiết như nguồn, đích, loại gói tin, dữ liệu payload và nhiều thông tin khác.
- Đánh giá Hiệu suất Mạng: Wireshark cung cấp thông tin về thời gian phản hồi (response time), độ trễ (latency), và các thống kê khác, giúp đánh giá hiệu suất của mạng.

- Phân tích Giao thức: Wireshark hỗ trợ nhiều giao thức mạng khác nhau. Bạn có thể xem và phân tích giao thức HTTP, TCP, UDP, IP, DNS, và nhiều giao thức khác.
- Điều tra Vấn đề Mạng: Khi xảy ra vấn đề mạng, Wireshark là một công cụ mạnh mẽ để phân tích và xác định nguyên nhân của sự cố.
- Bảo mật Mạng: Wireshark có thể được sử dụng để phát hiện các hoạt động độc hại trên mạng. Nó cho phép bạn xem gói tin để phát hiện các tấn công mạng, như phishing hoặc kiểm soát truy cập không được ủy quyền.
- Giáo dục và Học tập: Wireshark là một công cụ hữu ích cho sinh viên, chuyên gia mạng, và người quan tâm đến việc hiểu rõ cách mạng hoạt động. Nó cung cấp một cách thức thực hành để nắm bắt và hiểu các khái niệm mạng.

1.2.4 Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Network Miner

NetworkMiner là một công cụ phân tích mạng dành cho Windows. Nó cho phép người dùng thu thập dữ liệu từ mạng và phân tích thông tin như các máy chủ, giao thức, trình duyệt web, và nhiều hơn nữa. NetworkMiner tự động phát hiện các hoạt động mạng như kết nối TCP, truy vấn DNS và nó cũng có thể hỗ trợ trong việc phát hiện và phân loại các tập tin được truyền qua mạng. Nó thường được sử dụng để phát hiện các mối đe dọa mạng và phân tích dữ liệu từ gói tin đã chụp.

Những điểm nổi bật của NetworkMiner phải kể đến:

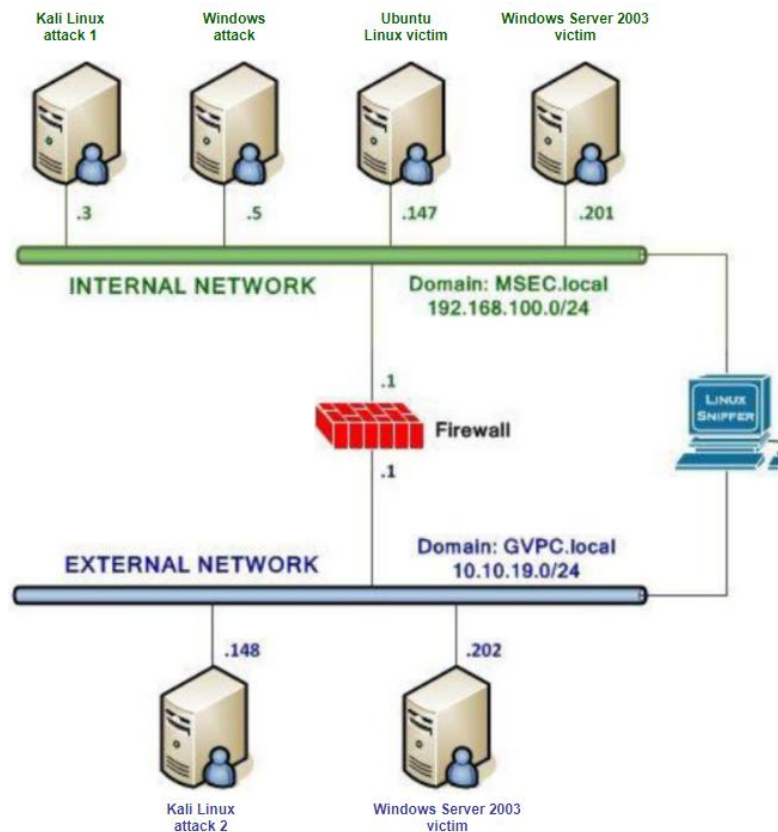
- Giám sát hầu như mọi gói tin trao đổi ra vào máy chủ, trong đó cho phép phát hiện ảnh, các file dữ liệu và tài khoản đăng nhập.
- Dữ liệu hiển thị ở dạng rất dễ hiểu.
- Dung lượng nhẹ (phiên bản 2.6 sau khi giải nén chỉ chiếm 47,9 MB), không cần cài đặt (chỉ cần tải về, giải nén là sử dụng được ngay) và rất dễ sử dụng.
- Có hai phiên bản miễn phí và pro (trả phí) để lựa chọn. Trong đó, phiên bản trả phí cho phép tìm kiếm trực tuyến thông tin về địa chỉ IP.
- Khả năng phân tích email trao đổi qua các giao thức SMTP, POP3 và IMAP.
- Nâng cấp khả năng phát hiện mật khẩu, phát hiện trao đổi dữ liệu qua giao thức FTP, những dấu hiệu bất thường trong trao đổi dữ liệu qua giao thức HTTP và HTTP/2.
- Nâng cấp khả năng tương thích với hệ điều hành Linux.
- Hỗ trợ phân tích các gói tin qua giao thức GRE, PPPoE, VXLAN, OpenFlow, MPLS và EoMPLS.

NetworkMiner là một công cụ phân tích mạng có khả năng thu thập dữ liệu từ gói tin mạng trên một giao diện cụ thể trên máy tính. Sau đó, nó phân tích các gói tin để trích xuất thông tin quan trọng như địa chỉ IP, tên miền, thông tin trình duyệt web và các tập tin được truyền qua mạng. Dữ liệu được hiển thị trên giao diện người dùng và có thể được lưu trữ dưới dạng tập tin PCAP để phân tích và thẩm định sau này.

CHƯƠNG 2. NỘI DUNG BÀI THỰC HÀNH

2.1 Chuẩn bị môi trường

- Cài đặt VMWare Workstation hoặc phần mềm ảo hóa khác.
- Kiểm tra lại các máy ảo đã thiết lập từ bài thực hành trước:



▪ Máy Kali Linux attack 1 trong mạng Internal	<ul style="list-style-type: none"> ▪ IP: 192.168.100.3 ▪ Mật khẩu root: password
▪ Máy Windows Server 2003 Victim trong mạng Internal	<ul style="list-style-type: none"> ▪ IP: 192.168.100.201 ▪ Mật khẩu root: password
▪ Máy Linux Victim trong mạng Internal	<ul style="list-style-type: none"> ▪ IP: 192.168.100.147 ▪ Mật khẩu root: password
▪ Máy pfSense Firewall	<ul style="list-style-type: none"> ▪ IP: 10.10.19.1, 192.168.100.1 ▪ Mật khẩu: admin/pfsense
▪ Máy Linux Attack trong mạng External	<ul style="list-style-type: none"> ▪ IP: 10.10.19.148 ▪ Mật khẩu root: password
▪ Máy Windows Server 2003 Victim trong mạng External	<ul style="list-style-type: none"> ▪ IP: 10.10.19.202 ▪ Mật khẩu root: password

- Máy trạm (Windows 10)

The screenshot shows a Windows 10 command prompt window with the following commands and output:

```
C:\Users\ThanhTam- B22DCAT253>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::d810:cfd1:8a94:9833%4
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Simultaneously, a separate Command Prompt window shows the execution of the following commands:

```
C:\Users\ThanhTam- B22DCAT253>date
The current date is: Mon 03/31/2025
Enter the new date: (mm-dd-yy)

C:\Users\ThanhTam- B22DCAT253>echo "Đinh Thị thanh Tam - B22DCAT253"
"Đinh Thị thanh Tam - B22DCAT253"
```

- Máy Kali Linux (Sniffer)

The screenshot displays a Kali Linux terminal window with the following commands and output:

```
kali@b22dcat253-DinhThiThanhTam: ~
File Actions Edit View Help
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ ifconfig -a

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::2e7a:e94f:892a:5974 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ef:4e:61 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 1825 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 6137 (5.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 248 bytes 19920 (19.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 248 bytes 19920 (19.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@b22dcat253-DinhThiThanhTam: ~
File Actions Edit View Help
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ date
Mon Mar 31 09:55:56 AM EDT 2025

(kali@b22dcat253-DinhThiThanhTam)-[~]
$ echo "Đinh Thị Thanh Tam - B22DCAT253"
```

- Máy chủ Windows 2019

The screenshot shows a Windows 2019 Administrator Command Prompt window with the following commands and output:

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::b77b:16ab:8ec4:1e0d%14
    IPv4 Address. . . . . : 192.168.100.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Simultaneously, a separate Administrator Command Prompt window shows the execution of the following commands:

```
C:\Users\Administrator>date
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>date
The current date is: Mon 03/31/2025
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo "Đinh Thị Thanh Tam - B22DCAT253"
"Đinh Thị Thanh Tam - B22DCAT253"

C:\Users\Administrator>
```

- Máy chủ Linux

The screenshot displays a Kali Linux terminal window with the following commands and output:

```
b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~
File Actions Edit View Help
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:62:44:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.3/24 brd 192.168.100.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe62:4497/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~
$

b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer: ~
File Actions Edit View Help
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ date
Mon Mar 31 11:13:55 AM EDT 2025

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ echo "Đinh Thị Thanh Tam - B22DCAT253"
Đinh Thị Thanh Tam - B22DCAT253

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$
```

- Đảm bảo các máy cần sử dụng đã được bật.

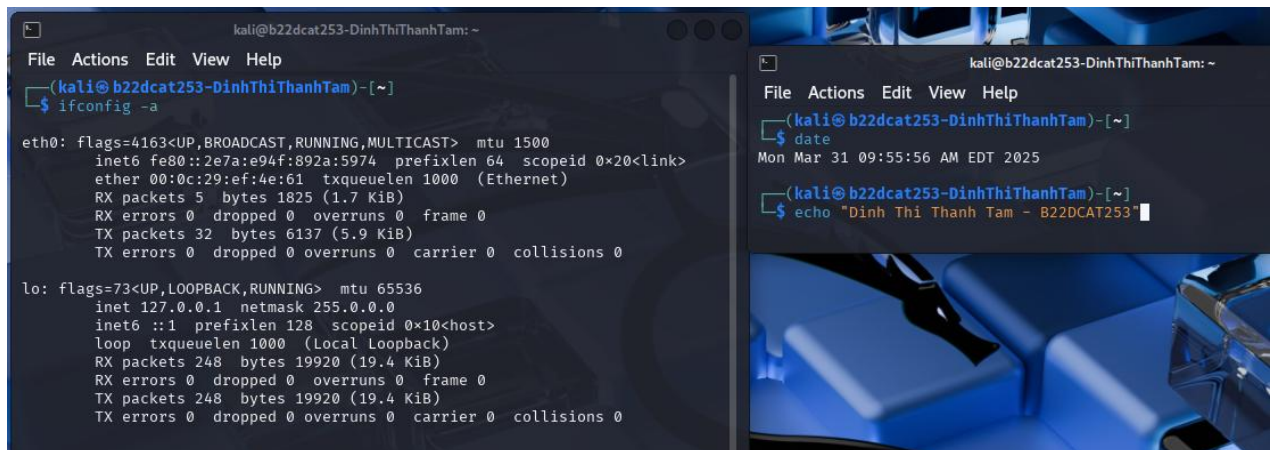
2.2 Các bước thực hiện

2.2.1 Sử dụng tcpdump để bắt gói tin

Bước 1: Xem tất cả các interfaces trong hệ thống

- Xem danh sách các interface trong Linux Sniffer

ifconfig -a



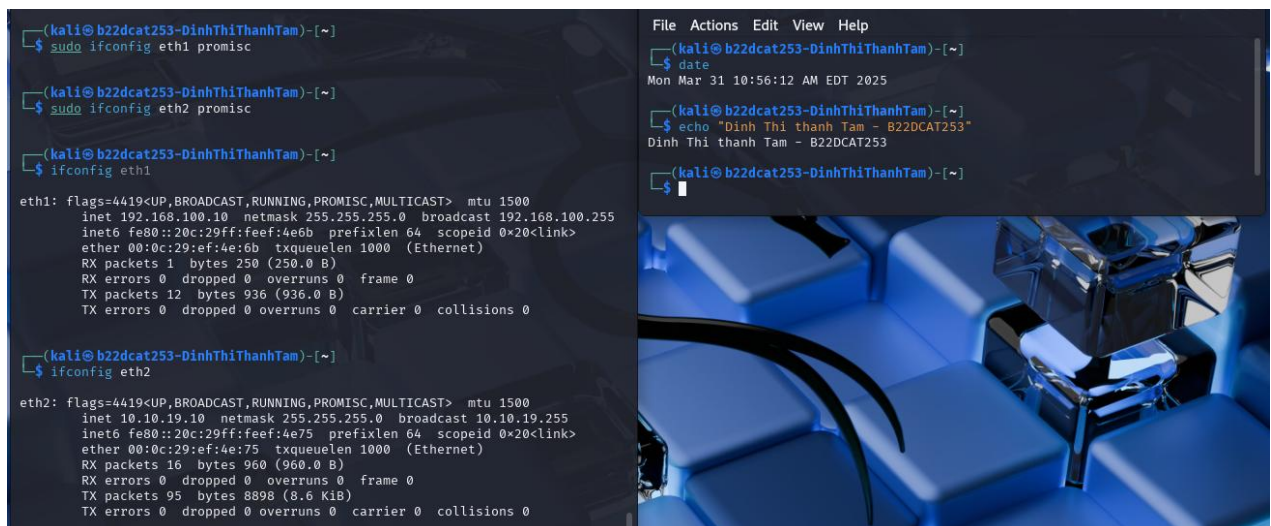
```
kali@b22dcat253-DinhThiThanhTam: ~  
File Actions Edit View Help  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ ifconfig -a  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet6 fe80::2e7a:e94f:892a:5974 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ef:4e:61 txqueuelen 1000 (Ethernet)  
    RX packets 5 bytes 1825 (1.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32 bytes 6137 (5.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 248 bytes 19920 (19.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 248 bytes 19920 (19.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@b22dcat253-DinhThiThanhTam: ~  
File Actions Edit View Help  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ date  
Mon Mar 31 09:55:56 AM EDT 2025  
  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
```

Bước 2: Kích hoạt interface (eth1, eth2) và khởi động tcpdump trên Windows Attack

sudo ifconfig eth1 up

sudo ifconfig eth2 up

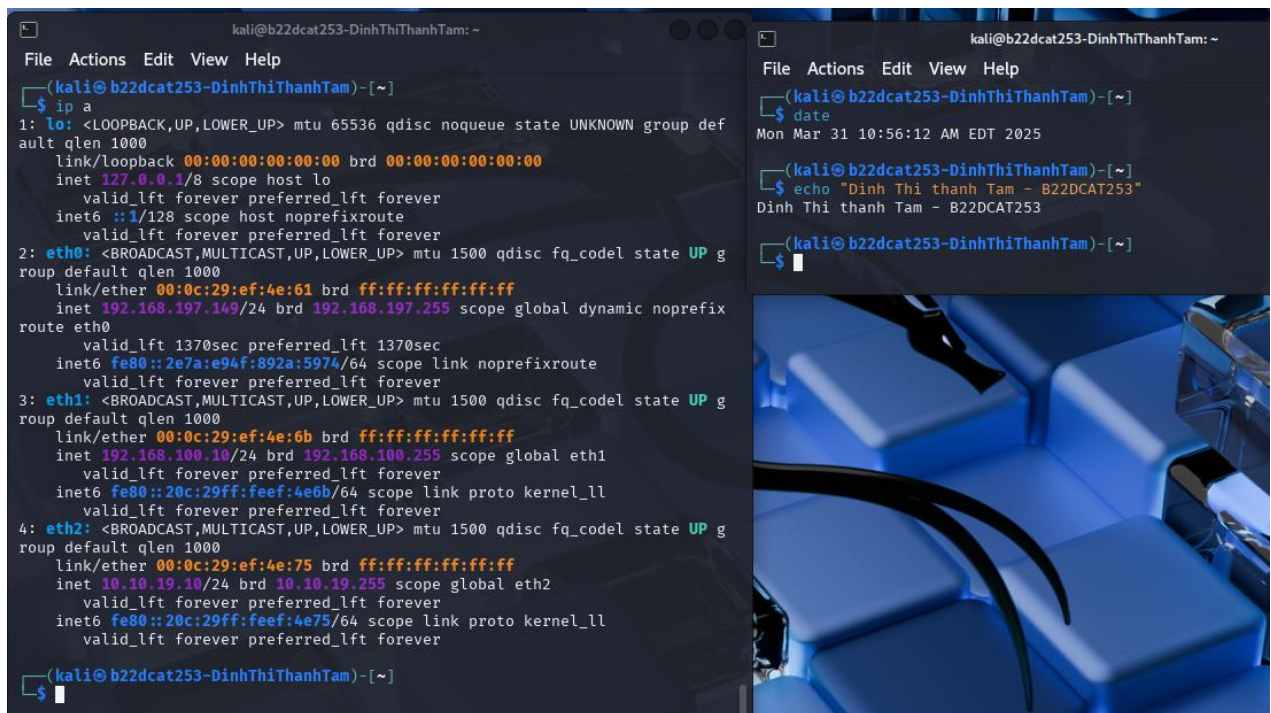
Bước 3: Kích hoạt interface và khởi động tcpdump trên Windows Attack



```
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ sudo ifconfig eth1 promisc  
  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ sudo ifconfig eth2 promisc  
  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ ifconfig eth1  
  
eth1: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500  
    inet 192.168.100.10 netmask 255.255.255.0 broadcast 192.168.100.255  
    inet6 fe80::20c:29ff:feef:4e6b prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ef:4e:6b txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 250 (250.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 12 bytes 936 (936.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ ifconfig eth2  
  
eth2: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500  
    inet 10.10.10.10 netmask 255.255.255.0 broadcast 10.10.10.255  
    inet6 fe80::20c:29ff:feef:4e75 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ef:4e:75 txqueuelen 1000 (Ethernet)  
    RX packets 16 bytes 960 (960.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 95 bytes 8898 (8.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@b22dcat253-DinhThiThanhTam: ~  
File Actions Edit View Help  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ date  
Mon Mar 31 10:56:12 AM EDT 2025  
  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$ echo "Dinh Thi thanh Tam - B22DCAT253"  
Dinh Thi thanh Tam - B22DCAT253  
  
(kali@b22dcat253-DinhThiThanhTam)-[~]  
$
```

Bước 4: Xem danh sách các interface trong Linux Sniffer sau khi kích hoạt interface

ifconfig -a

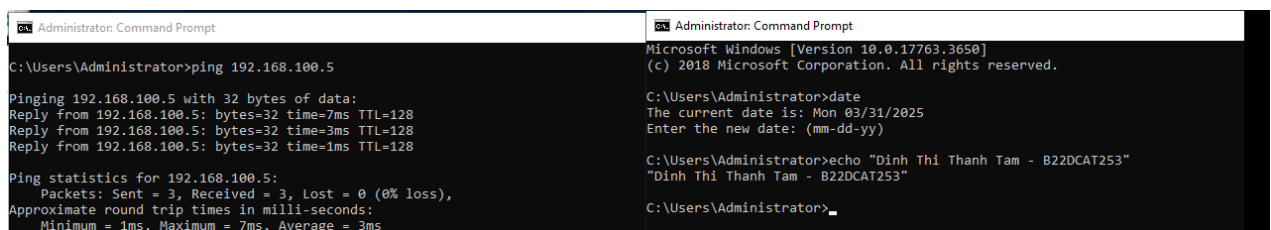


➔ Thấy eth1 đã kích hoạt với địa chỉ: 192.168.100.10

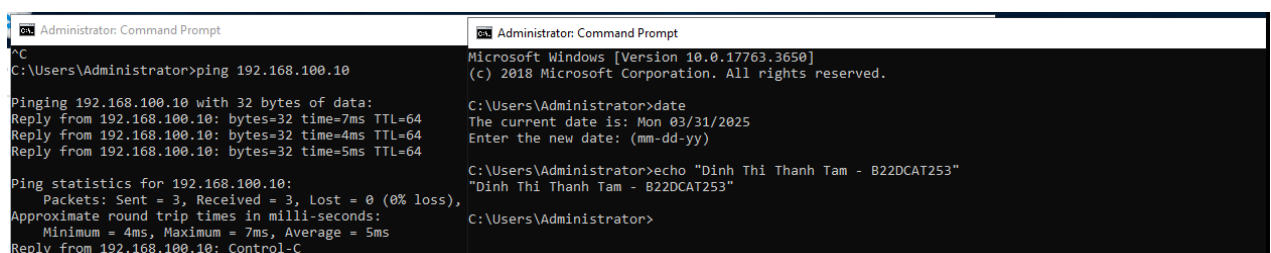
➔ Thấy eth2 đã kích hoạt với địa chỉ: 10.10.19.10

Bước 5: Trên Windows Server 2003, gửi tín hiệu ping đến giải mạng internal

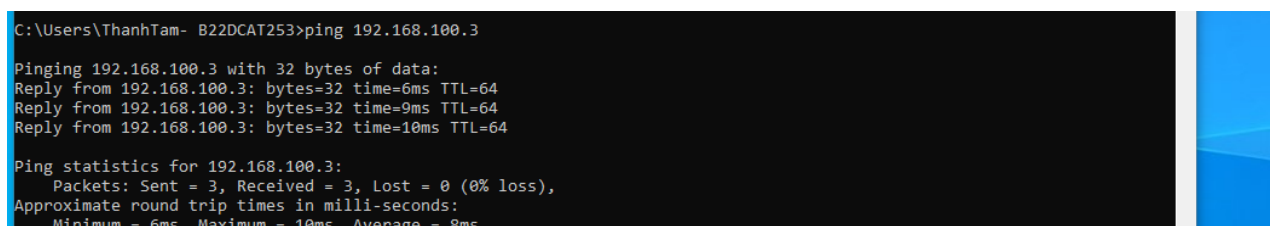
- Ping đến win 10



- Ping đến sniffer



- Ping đến kali linux



Bước 6: Bắt gói tin trên dải mạng 192.168.100.0/24 và lưu vào file capture_eth1.pcap

- Thời gian chờ dữ liệu trong khoảng 5 phút

Bước 7: Trên Windows Server 2003, gửi tín hiệu ping đến giải mạng external

- Ping đến snifer mạng eternal

Bước 8: Bắt gói tin trên dải mạng 10.10.19.0/24 và lưu vào file capture_eth2.pcap

Bước 9: Kiểm tra và lưu file bắt gói tin

`ls -l *.pcap`

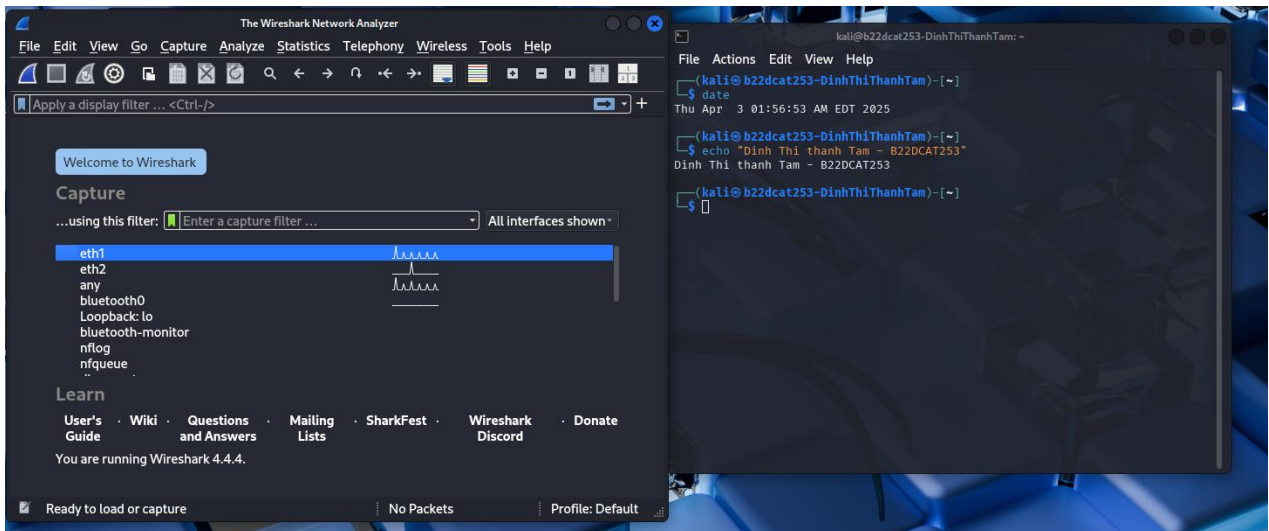
```
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ ls
capture_eth0.pcap  capture.pcap  Downloads  Public  Templates
capture_eth1.pcap  Desktop      Music      Templates
capture_eth2.pcap  Documents   Pictures   Videos

(kali@b22dcat253-DinhThiThanhTam)-[~]
$ date
Thu Apr  3 05:50:28 AM EDT 2025

(kali@b22dcat253-DinhThiThanhTam)-[~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
```

2.2.2 Sử dụng Wireshark để phân tích gói tin trên dải mạng 192.168.100.0

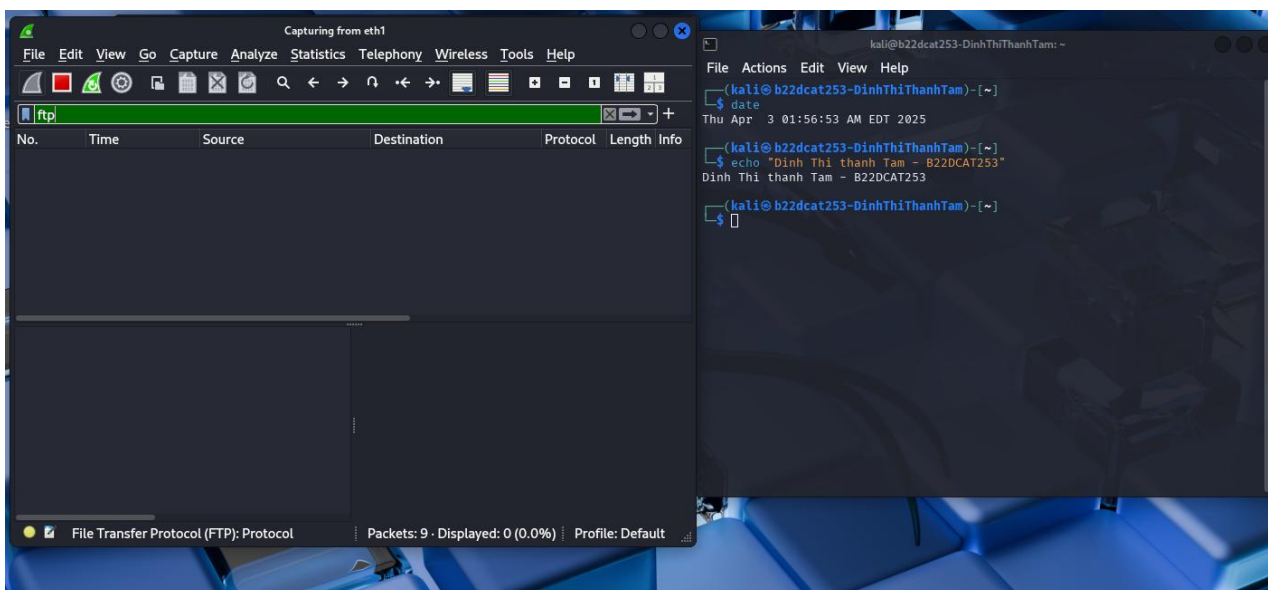
Bước 1: Tải và cài đặt Wireshark: Wireshark Download



Bước 2: Khởi động Wireshark, chọn eth1 để bắt gói tin trên dải mạng 192.168.100.0

- Để xem các gói tin FTP trong danh sách
- Vào Filter, nhập:

ftp



Bước 3: Thực hiện kết nối FTP từ Windows 10

[ftp 192.168.100.201](#)


```

C:\Users\ThanhTam- B22DCAT253>ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.100.201:(none)): administrator
331 Password required
Password:
230 User logged in.
ftp>

C:\Users\ThanhTam- B22DCAT253>date
The current date is: Thu 04/03/2025
Enter the new date: (mm-dd-yy)

C:\Users\ThanhTam- B22DCAT253>echo "Dinh Thi Thanh Tam - B22DCAT253"
"Dinh Thi Thanh Tam - B22DCAT253"

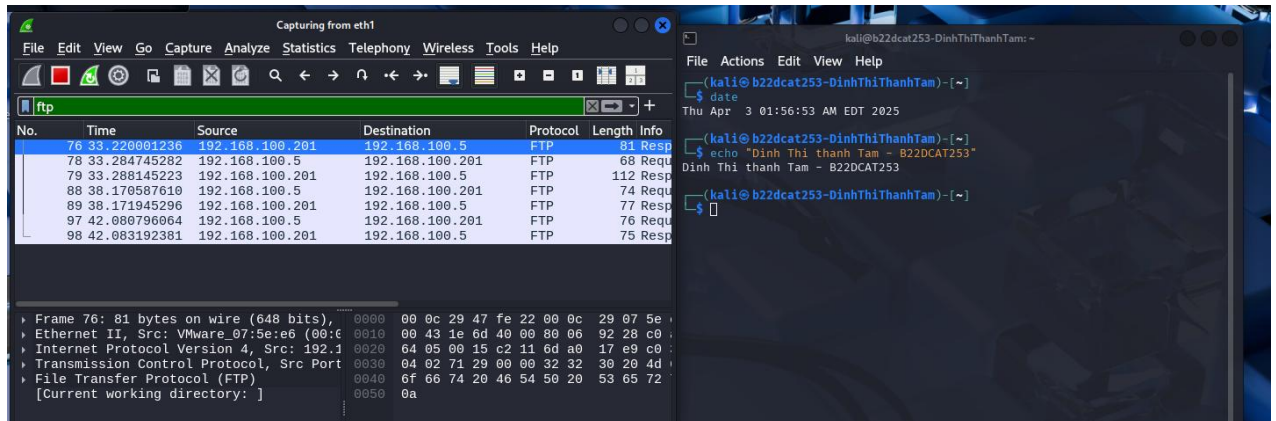
C:\Users\ThanhTam- B22DCAT253>

```

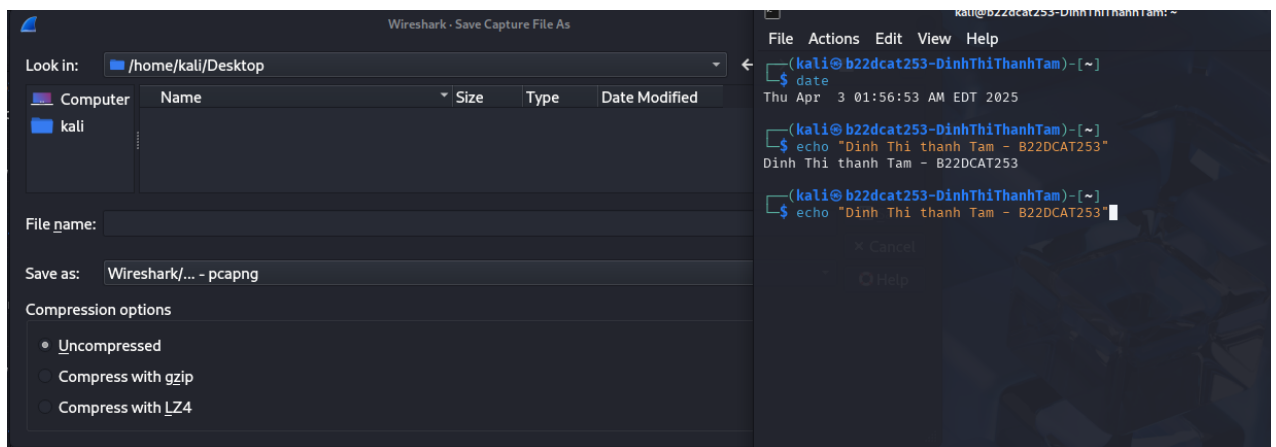
➔ Kết nối ftp thành công, tiến hành dùng wireshark để bắt gói tin

Bước 4: Danh sách các gói tin được bắt theo giao thức FTP

- Yêu cầu ftp giữa 2 mạng 192.168.100.5 (window 10) và máy 192.168.100.201 (Window Server)



Lưu kết quả vào file pcap



2.2.3 Sử dụng Wireshark để phân tích gói tin trên dải mạng 10.10.19.0

Bước 1: Khởi động Wireshark , chọn eth2 để bắt gói tin trên dải mạng 10.10.19.0

- Để xem các gói tin FTP trong danh sách
- Vào Filter, nhập:

ftp

Bước 2: Trên máy Window Server 2003 victim, kết nối với ftp server

ftp 10.10.19.202

```

(kali@b22dcat253-DinhThiThanhTam)-[~]
$ ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
Name (10.10.19.202:kali): administrator
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> exit
221 Goodbye.

(kali@b22dcat253-DinhThiThanhTam)-[~]
$

```

```

kali@b22dcat253-DinhThiThanhTam: ~
File Actions Edit View Help
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ date
Thu Apr 3 01:56:53 AM EDT 2025
(kali@b22dcat253-DinhThiThanhTam)-[~]
$ echo "Dinh Thi thanh Tam - B22DCAT253"
Dinh Thi thanh Tam - B22DCAT253
(kali@b22dcat253-DinhThiThanhTam)-[~]
$

```

Bước 3: Danh sách các gói tin được bắt theo giao thức FTP

- Yêu cầu ftp giữa 2 mạng 10.10.19.10 (window 10) và máy 10.10.19.202 (Window Server)

No.	Time	Source	Destination	Protocol	Length	Info
12	9.823009005	10.10.19.10	10.10.19.202	FTP	60	Req
13	9.824423318	10.10.19.202	10.10.19.10	FTP	70	Res
14	9.824773392	10.10.19.10	10.10.19.202	FTP	60	Req
15	9.826307667	10.10.19.202	10.10.19.10	FTP	88	Res
16	9.826308180	10.10.19.202	10.10.19.10	FTP	72	Res
17	9.826308285	10.10.19.202	10.10.19.10	FTP	107	Res
18	9.826466146	10.10.19.10	10.10.19.202	TCP	54	579
19	9.826743827	10.10.19.202	10.10.19.10	FTP	61	Res
20	9.827131189	10.10.19.202	10.10.19.10	FTP	91	Res
21	9.827532728	10.10.19.10	10.10.19.202	TCP	54	579

```

Frame 1: 74 bytes on wire (592 bits), 70 captured (568 bits) on eth2
Ethernet II, Src: VMware_ef:4e:75 (00:0c:29:07:5e:e6), Dst: 08:00:0c:29:07:5e:00:0c
Internet Protocol Version 4, Src: 10.10.19.10, Destination: 10.10.19.202
Transmission Control Protocol, Src Port: 579, Dst Port: 21

```

Lưu kết quả vào file pcap tương ứng

2.2.4 Sử dụng Network Miner để phân tích gói tin

Bước 1: Cài đặt Network Miner

- Trên máy Window Attack cài đặt Network Miner từ trang chủ:
<https://www.netresec.com/?page=NetworkMiner>

Bước 2: Khởi động Network Miner trên Windows Attack

```

NetworkMiner 2.9.0
File Tools Help
--- Select a network adapter in the list ---
Socket: VPN Client Adapter - VPN (disconnected)
Socket: Intel(R) Q2574L Gigabit Network Connection #2 (10.10.19.5)
Socket: Bluetooth Device (Personal Area Network) (disconnected)
Socket: Software Loopback Interface 1 (:1)
Socket: Software Loopback Interface 1 (127.0.0.1)

C:\Users\ThanhTam- B22DCAT253>date
The current date is: Thu 04/03/2025
Enter the new date: (mm-dd-yy)

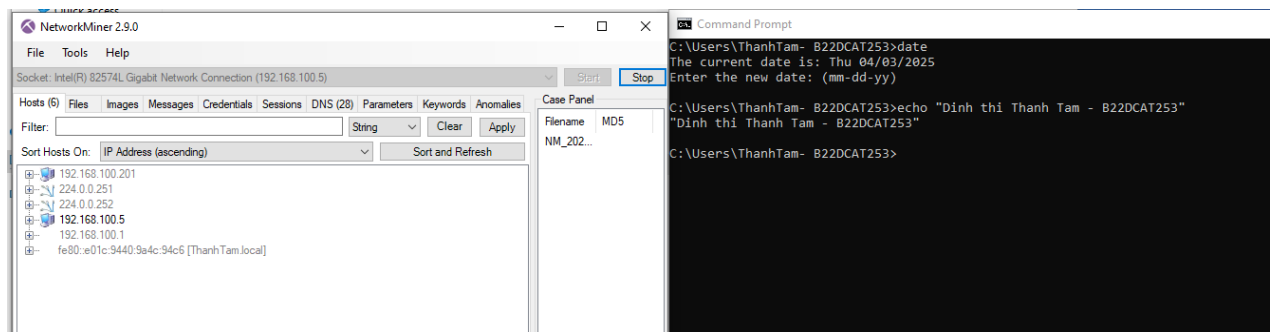
C:\Users\ThanhTam- B22DCAT253>echo "Dinh thi Thanh Tam - B22DCAT253"
"Dinh thi Thanh Tam - B22DCAT253"

C:\Users\ThanhTam- B22DCAT253>

```

Bước 3: Chọn Card mạng Intel® PRO/1000MT Connection (192.168.100.5) và bắt đầu bắt gói tin.

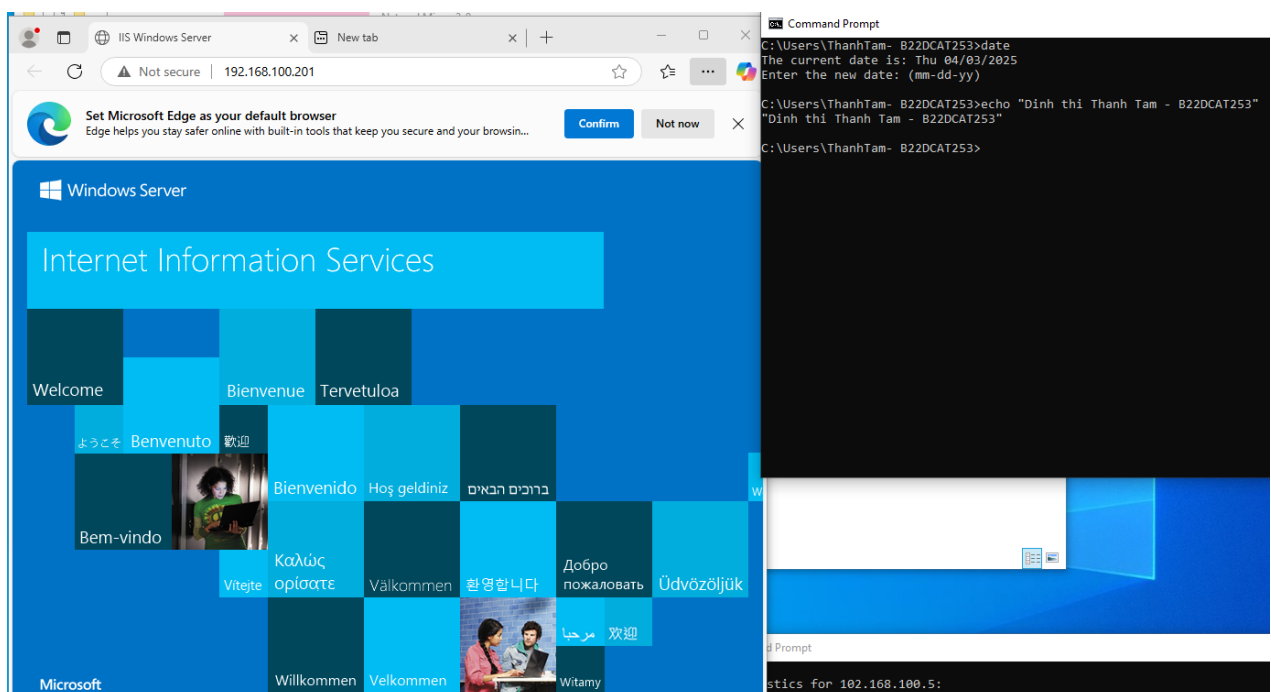
- Nhấn "Start" để bắt đầu thu thập dữ liệu mạng.



- Địa chỉ IP thu thập được:
 - 192.168.100.201
 - 192.168.100.5 (chính là máy đang chạy NetworkMiner).
 - Một số địa chỉ multicast (224.0.0.251, 224.0.0.252)
 - Địa chỉ IPv6 (fe80::81c:s440:9a4c:94c5)

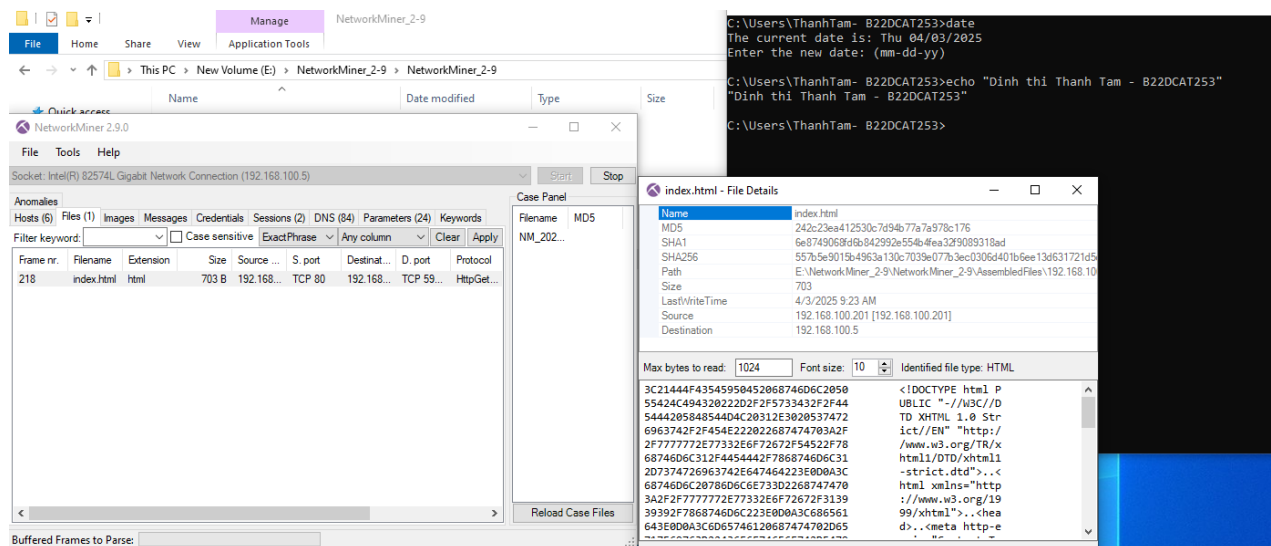
➔ Điều này cho thấy NetworkMiner đã bắt được các gói tin từ mạng nội bộ, chứng tỏ card mạng đang hoạt động và có dữ liệu truyền tải.

Bước 4: Kết nối đến trang web của Windows 2019 Server Internal: <http://192.168.100.201/>



- Dừng bắt gói tin và kiểm tra dữ liệu trong Network Miner

Bước 5: Trong Network Miner, chọn File/ index.html để xem dữ liệu gói tin vừa bắt được



- Cửa sổ "File Details" hiển thị thông tin như:
 - Tên tệp: index.html
 - MD5 Hash: Một giá trị dùng để xác định tính toàn vẹn của tệp.
 - SHA256 Hash: Một hàm băm mạnh hơn dùng để kiểm tra sự thay đổi của tệp.
 - Đường dẫn: Tệp này được trích xuất từ một luồng dữ liệu trong NetworkMiner.
 - Nội dung: Một phần dữ liệu của tệp HTML hiển thị trong khung.

KẾT LUẬN

- Thu được kết quả bắt gói tin và các file pcap thông qua tcpdump
- Sử dụng Wireshark để bắt và lọc ra được các gói tin ftp, các file pcap tương ứng
- Bắt được các dữ liệu trong file index.html

TÀI LIỆU THAM KHẢO

- [1] Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021
- [2] <https://www.tcpdump.org/index.html#documentation>
- [3] https://www.wireshark.org/docs/wsug_html/
- [4] <https://docs.securityonion.net/en/2.3/networkminer.html#>